

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: **Allan et al.**

\$ Group Art Unit: **2154**

Serial No.: **09/583,958**

\$

\$ Examiner: **Nguyen, D.**

Filed: **05/31/2000**

\$

\$ Atty Docket #: **AUS9-2000-0254-US1**

For: **Method and system for  
dynamic update of an  
application monitoring agent  
using a non-polling mechanism**

5

**APPELLANT'S BRIEF**  
**IN RESPONSE TO OFFICE ACTION UNDER 37 C.F.R. § 41.37**

10       This brief is filed in support of the Notice of Appeal,  
filed xx/xx/xxxx, and which appeals the rejection of claims 1-25  
from the decision of the examiner dated xx/xx/xxxx.

**I. REAL PARTY IN INTEREST**

The real party in interest in this appeal is International Business Machines Corporation (IBM).

5 **II. RELATED APPEALS AND INTERFERENCES**

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

10

**III. STATUS OF CLAIMS**

**III.A. TOTAL NUMBER OF CLAIMS**

A total of 21 claims remain pending in this application.

15

**III.B. STATUS OF ALL CLAIMS IN THIS APPLICATION**

Claims canceled: None.

Claims withdrawn: None.

Claims pending: 1-21.

20

Claims allowed: None.

Claims rejected: 1-21.

Claims objected to: None.

**III.C. CLAIMS ON APPEAL**

25

The claims on appeal are: 1-21.

**IV. STATUS OF AMENDMENTS**

No after-final amendments have been filed.

## V. SUMMARY OF CLAIMED SUBJECT MATTER

### V.A. INDEPENDENT CLAIM 1

Claim 1 is directed to a method for updating operational  
5 parameters (FIG. 2, 222; page 14, line 14) of a monitoring agent  
(220; page 14, line 10) on a client (201; page 13, line 20) in a  
distributed data processing system (200; page 13, line 18). The  
monitoring agent monitors characteristics of at least one  
application executing on a server (202; page 13, line 19) in the  
10 distributed data processing system.

The monitoring agent is configured to perform the following  
steps:

a first step of filtering, by the monitoring agent (FIG. 3,  
step 302; page 17, line 24), network data (service requests 206;  
15 service responses 208; configuration/policy updates 210; page 13)  
from the client to the server;

a second step of determining, by the monitoring agent (step  
310--page 18, line 2; FIG. 4, step 458--page 21, line 16),  
whether an outgoing transaction in the network data  
20 (configuration/policy updates 210; page 13, line 29) is addressed  
such that an application on the server receives the outgoing  
transaction as a request to change the operational parameters of  
the monitoring agent; and

a third step of sending a request from the monitoring agent  
25 to the server to send to the monitoring agent an update of the  
operational parameters of the monitoring agent (step 312--page  
18, line 6; step 460--page 21, line 18) in response to a positive  
determination that the outgoing transaction is addressed such  
that an application on the server receives the outgoing  
30 transaction as a request to change the operational parameters of  
the monitoring agent.

VI. Grounds of rejection to be reviewed on appeal

VI.A. Obviousness over Pandya et al. in view of Lin et al.

Whether claims 1, 2, 5-9, 12-16, and 19-21 are  
unpatentable under 35 U.S.C. § 103(a) over Pandya et al.,  
"Software, systems, and methods for managing a distributed  
network", U.S. Patent No. 6,671,724 B1, filed 03/21/2000,  
issued 12/30/2003, in view of Lin et al., "Network  
management system based on passive monitoring and proactive  
management for formulation behavior state transition  
models", U.S. Patent Number 6,405,250 B1, filed 01/25/1999,  
issued 06/11/2002.

## VII. ARGUMENTS

VII.A. Was 35 U.S.C. § 103(a) properly applied in a rejection of claims 1, 2, 5-9, 12-16, and 19-21 as being unpatentable over Pandya et al. in view of Lin et al.?

All of the pending independent claims have been rejected, at least in part, over a combination of the disclosure of Pandya et al. and Lin et al.; each of the independent claims has one or more common elements against which the rejection applies certain portions of Pandya et al. and Lin et al.. However, Appellant asserts that there is at least one element of each independent claim that is not shown in Pandya et al. and Lin et al. nor provided by a combination of Pandya et al. and Lin et al., thereby causing these obviousness rejections to be deficient.

Hence, claims 1-21 stand and fall together as a single group. The rejection of all independent claims is based on the rejection of independent claim 1. Therefore, for purposes of this argument, Appellant argues for the patentability of claims 1-21 of the present invention using claim 1 as an exemplary claim.

The majority of the Office action is devoted to the rejection of independent claim 1, which addresses the first two elements or steps of method claim 1 by referencing Pandya et al. and then addresses the third element or step of method claim 1 by referencing Lin et al.. Claim 1 reads as follows:

1. A method for updating operational parameters of a monitoring agent on a client in a distributed data processing system, the monitoring agent monitoring characteristics of at least one application executing on a server in the distributed data processing system, the method comprising the steps of:

filtering, by the monitoring agent, network data from the client to the server;

determining, by the monitoring agent, whether an outgoing transaction in the network data is addressed such that an application on the server receives the outgoing transaction as a request to change the operational parameters of the monitoring agent; and

in response to a positive determination that the outgoing transaction is addressed such that an application on the server receives the outgoing transaction as a request to change the operational parameters of the monitoring agent, sending a request from the monitoring agent to the server to send to the monitoring agent an update of the operational parameters of the monitoring agent.

The first part of the rejection of claim 1 states on page 5, first paragraph, of the final Office action:

filtering, by the monitoring agent, network data from the client to the server [col 10, lines 12-52];

determining, by the monitoring agent, whether an outgoing transaction in the network data is addressed such that an application on the server receives the outgoing transaction as a request to change the operational parameters of the monitoring agent [col 8, lines 46-64; col 11, lines 24-35].

The first portion of Pandya et al. that is cited by the rejection reads as follows:

As seen in FIG. 6, agent 70 is interposed between application program 122 and a communications protocol layer for providing end-to-end data transmission, such as transport layer 124 of communications protocol stack 92. Typically, the agent modules of the present invention are used with network devices that employ layered communications software adhering to either the OSI or TCP/IP-based protocol models. Thus, agent 70 is depicted as "interposed," i.e. in a data path, between an application program and a transport protocol layer. However, it will be appreciated by those skilled in the art that the invented agent may be used with protocol software not adhering to either the OSI or TCP/IP models, but that nonetheless includes a protocol layer providing transport functionality, i.e. providing for end-to-end data transmission.

Because of the depicted position within the data path, agent 70 is able to monitor network traffic and obtain information that is not available by hooking into transport layer 124 or the layers below the transport layer. At the higher layers, the available data is richer and more detailed. Hooking into the stack at higher layers allows the network to become more "application-aware" than is possible when monitoring occurs at the transport and lower layers.

The agent modules may be interposed at a variety of points between application program 122 and transport layer 124. Specifically, as shown in FIGS. 7 and 8, agent 70 may be associated with a client computer so that it is adjacent an application programming interface (API) adapted to provide a standardized interface for application program 122 to access a local operating system (not shown) and communications stack 92. In FIG. 7, agent 70 is adjacent a winsock API 128 and interposed between application program 122 and the winsock interface. FIG. 8 shows an alternate configuration, in which agent 70 is again adjacent the winsock interface, but the winsock interface is interposed between application program 122 and agent 70. With either configuration, the agent is interposed between the transport layer 124 of communications stack 92 and is adapted to directly monitor data received by or sent from the winsock interface.--(column 10, lines 12-52).

Hence, the fact that Pandya et al. discloses a monitoring agent (agent module) that filters network traffic is not disputed.

However, the second and third portions of Pandya et al. that are cited by the rejection read as follows (emphasis added):

For example, continuous media applications such as IP telephony have certain bandwidth requirements for optimum performance, and are particularly sensitive to network jitter and delay. Policies could be written to specify a desired level of service, including bandwidth requirements and threshold levels for jitter and delay, for client computers attempting to run IP telephony applications. The policies would further direct the agents and control modules to attempt to provide the specified level of service. Security checking could also be included to ensure that the particular user or client computer was permitted to run the application. In the event that the specified service level could not be provided, the requesting user could be provided with a message indicating that the resources for the request

were not available. The user could also be offered various options, including proceeding with a sub-optimal level of service, placing a conventional telephone call, waiting to perform the task until a later time, etc.--(c. 8, l. 46-64).

5 To provide the specified network service level, traffic control module 132 may maintain a queue or plurality of queues. When data is sent from the client to the network, or from the network to the client, redirector module 130 intercepts the data, and **traffic module 132 places the individual units of data in the appropriate queue.** The control points may be configured to periodically provide traffic control commands, which may include the QoS parameters and service specifications discussed above. In response, **traffic control module 132 controls the passing of data into, through or out of the queues in order to provide the specified service level.**--(c. 11, lines 24-35).

It should be apparent that Pandya et al. does not disclose the second element of claim 1, i.e. "determining, by the monitoring agent, whether an outgoing transaction in the network data is addressed such that an application on the server receives the outgoing transaction as a request to change the operational parameters of the monitoring agent". At most, Pandya et al. mentions in the second copied portion that "policies would further direct the agents and control modules to attempt to provide the specified level of service"; it may be fairly assumed from this statement that parameters are sent to the agent modules in accordance with the policies. However, the act of sending parameters to the agent modules is not equivalent nor analogous to the feature in the present application in which the monitoring agent scans the network traffic for a particular type of transaction that is being sent to a server in order to request that the server subsequently change the operational parameters of the monitoring agent. The third copied portion of Pandya et al. states that a traffic control module "controls the passing of data into, through or out of the queues". Again, this feature is



not equivalent or analogous to the claimed feature in the present application against which it was applied, i.e. the second element of claim 1. Hence, Pandya et al. does not have any features that are even remotely analogous to the second element of claim 1.

5 The second part of the rejection of claim 1 specifically states that Pandya et al. does not disclose the third element of claim 1 and then states on page 5, sixth paragraph of the final Office action, that Lin et al. discloses the third element; the rejection reads:

10 in response to a positive determination that the outgoing transaction is addressed such that an application on the server receives the outgoing transaction as a request to change the operational parameters of the monitoring agent, sending a request from the monitoring agent to the  
15 server to send to the monitoring agent an update of the operational parameters of the monitoring agent [col 7, lines 37-50; and col 8, lines 29-38].

20 The portions of Lin et al. that are cited against the third element by the rejection read as follows (emphasis added):

In addition to a database 451 which stores the behavior transition model for the NE associated with MA 450, MA 450 also includes a report filter 452 and an action enforcer 453. Report filter 452 receives raw MIB data, such as  
25 counter values and alarms from the associated network element and **uses the behavior model in database 451 to filter out unnecessary reporting details. MIB values that are potentially of interest to NMS 120 based on the current status of the NE associated with MA 450 are then aggregated and forwarded to NMS 120 through communicator 454.** On the  
30 other hand, **action enforcer 453 receives action requests from NMS 120 via communicator 454 and processes them.** The nature of the requests includes reconfiguring the network element, acquiring specific MIB values, or updating report  
35 filtering policies.--(column 7, lines 37-50).

Report filter 452 also receives NE generated alarms. For each alarm received, report filter 452 first saves the alarm information in a log file at step 531, then consults its current reporting policies in database 451 to decide if  
40 NMS 120 is interested in the alarm at step 532. **Depending**

on the outcome of the decision box step 532, report filter 452 either forwards the alarm information to communicator 454 at step 533, or proceeds back to the beginning of the event loop at step 502. Report filter 452 also loops back to step 502 at the end of steps 513, 523, and 533.--(column 8, lines 29-38).

It is not clear what features of the system that is disclosed in Lin et al. is meant to be applied against the claimed feature of the present invention because the rejection merely references multiple portions of text in Lin et al. without discussing the disclosed features. At most, Lin et al. discloses filtering of data, accumulation of certain data for forwarding to another entity, and receiving requests to perform certain actions.

However, it should be apparent that Lin et al. does not disclose the third element of claim 1, notwithstanding the argument in the rejection to the contrary; again, the third element of independent claim 1 reads:

in response to a positive determination that the outgoing transaction is addressed such that an application on the server receives the outgoing transaction as a request to change the operational parameters of the monitoring agent, sending a request from the monitoring agent to the server to send to the monitoring agent an update of the operational parameters of the monitoring agent.

Hence, Lin et al. does not have any features that are even remotely analogous to the third element of claim 1.

The motivational statement in the rejection is completely generic with respect to network traffic monitoring tools. The rejection states: "It would have been obvious to a person skilled in the art at the time the invention was made to combine the teaching of Pandya and Lin because Lin's teaching of monitoring agent sending request [sic] would allow reduce network traffic [sic] to prevent congestion in a communication network". As should be apparent, the motivational statement does not link any

particular characteristic from the teachings of Lin et al. into the teachings of Pandya et al.; there is no argument as to why someone would particularly look to the teachings of Lin et al. for something lacking in the teachings of Pandya et al., and  
5 there is no argument as to how an element from the system of Lin et al. could be integrated into the system of Pandya et al..

Appellant admits that both Pandya et al. and Lin et al. disclose distributed monitoring agents. However, these types of systems were admitted as prior art and were distinguished in the  
10 present application. Moreover, neither Pandya et al. nor Lin et al. disclose the operation of sending a request from a monitoring agent to a server for operational parameters for the monitoring agent, which is specifically recited in method claim 1 as happening when the agent detects an outgoing transaction to the  
15 server to change its operational parameters, or more generally in method claim 6, when the agent detects an outgoing transaction to the server. The present invention is directed to a specific process for the exchange of configuration information between a management server and the distributed monitoring agents; this  
20 exchange is triggered by a certain class of events that are detected by a monitoring agent, which is not shown in either Pandya et al. nor Lin et al. nor in a hypothetical combination of the disclosure of these references.

25 Rejections are deficient with respect to requirements for a proper obviousness rejection

Pandya et al. clearly fails to show a feature of the present invention as currently claimed and as asserted by the rejection, thereby rendering Pandya et al. incapable of being used as a  
30 primary reference as argued by the current rejection. In addition, Lin et al. clearly fails to show a feature of the

present invention as currently claimed and as asserted by the rejection, thereby rendering Lin et al. incapable of being used as a secondary reference as argued by the current rejection. Moreover, the hypothetical combination of Lin et al. and Lin et al. fail to show the claimed features. As should be recognized, because both the primary and secondary references in the rejection fail to disclose the claimed features against which the references were applied, and because the references fail to be combinable to produce this feature, the rejection fails to fulfill the requirements of a proper obviousness argument.

With respect to claims 1-21 of the present patent application, Appellant respectfully submits that the applied references cannot be combined to produce the claimed invention. Hence, a rejection of claims 1-21 cannot be based upon the cited prior art to establish a *prima facie* case of obviousness. Therefore, a rejection of the claims under 35 U.S.C. § 103(a) has been shown to be improper and insupportable in view of the cited prior art, and claims 1-21 are patentable over the applied references. For this and other reasons, Appellant argues that the position of the Examiner should be reversed and that the rejection of claims 1-21 should not be upheld.

## VIII. CLAIMS APPENDIX

1. A method for updating operational parameters of a monitoring agent on a client in a distributed data processing system, the  
5 monitoring agent monitoring characteristics of at least one application executing on a server in the distributed data processing system, the method comprising the steps of:

filtering, by the monitoring agent, network data from the client to the server;

10 determining, by the monitoring agent, whether an outgoing transaction in the network data is addressed such that an application on the server receives the outgoing transaction as a request to change the operational parameters of the monitoring agent; and

15 in response to a positive determination that the outgoing transaction is addressed such that an application on the server receives the outgoing transaction as a request to change the operational parameters of the monitoring agent, sending a request from the monitoring agent to the server to send to the monitoring  
20 agent an update of the operational parameters of the monitoring agent.

2. The method of claim 1 further comprising:

receiving, at the monitoring agent, the update of the operational parameters of the monitoring agent; and

storing updated operational parameters on the client in a manner accessible to the monitoring agent.

3. The method of claim 1 further comprising:

parsing the outgoing transaction for a Uniform Resource Identifier (URI);

matching the URI with a URI stored as an operational parameter of the monitoring agent on the client; and

providing an indication that the outgoing transaction is addressed such that the server receives the outgoing transaction as a request to change the operational parameters of the

monitoring agent.

4. The method of claim 3, wherein the URI is a Uniform Resource Locator (URL) embedded within a Hypertext Transport Protocol (HTTP) request.

5. The method of claim 1, wherein the request for an update of the operational parameters of the monitoring agent is addressed with a URI stored as an operational parameter of the monitoring agent on the client.

5

6. A method for updating operational parameters of a monitoring agent on a client in a distributed data processing system, the monitoring agent monitoring characteristics of at least one application executing on a server in the distributed data processing system, the method comprising the steps of:

filtering, by the monitoring agent, network data from the client to the server;

determining, by the monitoring agent, whether an outgoing transaction in the network data is addressed such that an application on the server receives the outgoing transaction; and

10 in response to a positive determination that the outgoing transaction is addressed such that an application on the server receives the outgoing transaction, sending a request from the monitoring agent to the server to send to the monitoring agent an

15 update of the operational parameters of the monitoring agent.



7. The method of claim 6 further comprising:

parsing the outgoing transaction for an Internet Protocol

(IP) address;

matching the IP address with an IP address stored as an

5 operational parameter of the monitoring agent on the client; and

determining that the outgoing transaction is addressed such  
that an application on the server receives the outgoing  
transaction.

8. A data processing system comprising a monitoring agent, the monitoring agent monitoring characteristics of at least one application executing on a server, the data processing system further comprising:

5 filtering means for filtering, by the monitoring agent, network data from the client to the server;

determining means for determining, by the monitoring agent, whether an outgoing transaction in the network data is addressed such that an application on the server receives the outgoing  
10 transaction as a request to change the operational parameters of the monitoring agent; and

sending means for sending, in response to a positive determination that the outgoing transaction is addressed such that an application on the server receives the outgoing  
15 transaction as a request to change the operational parameters of the monitoring agent, a request from the monitoring agent to the server to send to the monitoring agent an update of the operational parameters of the monitoring agent.

9. The data processing system of claim 8 further comprising:  
receiving means for receiving, at the monitoring agent, the  
update of the operational parameters of the monitoring agent; and  
storing means for storing updated operational parameters on  
5 the client in a manner accessible to the monitoring agent.

10. The data processing system of claim 8 further comprising:  
parsing means for parsing the outgoing transaction for a  
Uniform Resource Identifier (URI);

10 matching means for matching the URI with a URI stored as an  
operational parameter of the monitoring agent on the client; and  
providing means for providing an indication that the  
outgoing transaction is addressed such that the server receives  
the outgoing transaction as a request to change the operational  
15 parameters of the monitoring agent.

11. The data processing system of claim 10, wherein the URI is a  
Uniform Resource Locator (URL) embedded within a Hypertext  
Transport Protocol (HTTP) request.

12. The data processing system of claim 8, wherein the request for an update of the operational parameters of the monitoring agent is addressed with a URI stored as an operational parameter of the monitoring agent on the client.

13. A data processing system comprising a monitoring agent, the monitoring agent monitoring characteristics of at least one application executing on a server, the data processing system further comprising:

5       filtering means for filtering, by the monitoring agent, network data from the client to the server;

          determining means for determining, by the monitoring agent, whether an outgoing transaction in the network data is addressed such that an application on the server receives the outgoing

10   transaction; and

          sending means for sending, in response to a positive determination that the outgoing transaction is addressed such that an application on the server receives the outgoing transaction, a request from the monitoring agent to the server to  
15   send to the monitoring agent an update of the operational parameters of the monitoring agent.

14. The data processing system of claim 13 further comprising:

parsing means for parsing the outgoing transaction for an Internet Protocol (IP) address;

matching means for matching the IP address with an IP

5 address stored as an operational parameter of the monitoring agent on the client; and

determining means for determining that the outgoing transaction is addressed such that an application on the server receives the outgoing transaction.

10

15. A computer program product on a computer readable medium for use in a data processing system for updating operational parameters of a monitoring agent on a client in the data processing system, the monitoring agent monitoring characteristics of at least one application executing on a server in the data processing system, the computer program product comprising:

instructions for filtering, by the monitoring agent, network data from the client to the server;

10 instructions for determining, by the monitoring agent, whether an outgoing transaction in the network data is addressed such that an application on the server receives the outgoing transaction as a request to change the operational parameters of the monitoring agent; and

15 instructions for sending, in response to a positive determination that the outgoing transaction is addressed such that an application on the server receives the outgoing transaction as a request to change the operational parameters of the monitoring agent, a request from the monitoring agent to the  
20 server to send to the monitoring agent an update of the operational parameters of the monitoring agent.

16. The computer program product of claim 15 further comprising:  
instructions for receiving, at the monitoring agent, the  
update of the operational parameters of the monitoring agent; and  
instructions for storing updated operational parameters on  
5 the client in a manner accessible to the monitoring agent.

17. The computer program product of claim 15 further comprising:  
instructions for parsing the outgoing transaction for a  
Uniform Resource Identifier (URI);

10 instructions for matching the URI with a URI stored as an  
operational parameter of the monitoring agent on the client; and  
instructions for providing an indication that the outgoing  
transaction is addressed such that the server receives the  
outgoing transaction as a request to change the operational  
15 parameters of the monitoring agent.

18. The computer program product of claim 17, wherein the URI is  
a Uniform Resource Locator (URL) embedded within a Hypertext  
Transport Protocol (HTTP) request.



19. The computer program product of claim 15, wherein the request for an update of the operational parameters of the monitoring agent is addressed with a URI stored as an operational parameter of the monitoring agent on the client.

20. A computer program product on a computer readable medium for use in a data processing system for updating operational parameters of a monitoring agent on a client in the data processing system, the monitoring agent monitoring characteristics of at least one application executing on a server in the data processing system, the computer program product comprising:

instructions for filtering, by the monitoring agent, network data from the client to the server;

10 instructions for determining, by the monitoring agent, whether an outgoing transaction in the network data is addressed such that an application on the server receives the outgoing transaction; and

instructions for sending, in response to a positive  
15 determination that the outgoing transaction is addressed such that an application on the server receives the outgoing transaction, a request from the monitoring agent to the server to send to the monitoring agent an update of the operational parameters of the monitoring agent.

21. The computer program product of claim 20 further comprising:

instructions for parsing the outgoing transaction for an  
Internet Protocol (IP) address;

instructions for matching the IP address with an IP address  
5 stored as an operational parameter of the monitoring agent on the  
client; and

instructions for determining that the outgoing transaction  
is addressed such that an application on the server receives the  
outgoing transaction.

10

**IX. Evidence appendix**

None.

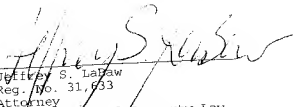
**5 X. Related proceedings appendix**

None.

**XI. Conclusion**

10 In view of the above arguments, it is respectfully urged  
that the rejection of the claims should not be sustained.

DATE: 10/24/06 Respectfully submitted,

15  
20   
25 Jeffrey S. LaFaw  
Reg. No. 31,633  
Attorney  
IBM Intellectual Property Law  
Austin, Texas 78758